Determinism and Computational Power of Real Measurement-based Quantum Computation

Simon Perdrix, Luc Sanselme

Determinism and Computational Power of Real Measurement-based Quantum Computation

Simon Perdrix *[1] and Luc Sanselme †[2]

[1]CNRS, LORIA, Université de Lorraine, Inria Project Team Carte, , France
[2]LORIA, CNRS, Université de Lorraine, Inria Project Team Caramba, Lycée Poincaré, France

Abstract

Measurement-based quantum computing (MBQC) is a universal model for quantum computation. The combinatorial characterisation of determinism in this model, powered by measurements, and hence, fundamentally probabilistic, is the cornerstone of most of the breakthrough results in this field. The most general known sufficient condition for a deterministic MBQC to be driven is that the underlying graph of the computation has a particular kind of flow called Pauli flow. The necessity of the Pauli flow was an open question. We show that Pauli flow is not necessary, providing several counter examples. We prove however that Pauli flow is necessary for determinism in the *real* MBQC model, an interesting and useful fragment of MBQC.

We explore the consequences of this result for real MBQC and its applications. Real MBQC and more generally real quantum computing is known to be universal for quantum computing. Real MBQC has been used for interactive proofs by McKague. The two-prover case corresponds to real-MBQC on bipartite graphs. While (complex) MBQC on bipartite graphs are universal, the universality of real MBQC on bipartite graphs was an open question. We show that real bipartite MBQC is not universal proving that all measurements of real bipartite MBQC can be parallelised leading to constant depth computations. As a consequence, McKague's techniques cannot lead to two-prover interactive proofs.

1 Introduction

Measurement-based quantum computing [18, 19] (MBQC for short) is a universal model for quantum computation. This model is not only very promising in terms of the physical realisations of the quantum computer [16, 21], MBQC has also several theoretical advantages, e.g. parallelisation of quantum operations [5, 3] (logarithmic separation with the traditional model of quantum circuits), blind quantum computing [2] (a protocol for delegated quantum computing), fault tolerant quantum computing [20], simulation [9], contextuality [17], interactive proofs [12, 2].

In MBQC, a computation consists of performing local quantum measurements over a large entangled resource state. The resource state is described by a graph – using the so-called graph state formalism [11]. The *tour de force* of this model is to tame the fundamental non-determinism of the quantum measurements: the number of possible outputs of a measurement-based computation on a given input is exponential in the number of measurements, and each of these branches of the computation is produced with an exponentially small probability. The only known technique to make such a fundamentally probabilistic

*simon.perdrix@loria.fr
†luc.sanselme@loria.fr

computation exploitable is to implement a correction strategy which makes the overall computation deterministic: it does not affect the probability for each branch of the computation to occur, but it guarantees that all the branches produce the same output.

The existence of a correction strategy relies on the structures of the entanglement of the quantum state on which the measurements are performed. Deciding whether a given resource state allows determinism is a central question in MBQC. Several sufficient conditions for determinism have been introduced. First in [6] the notion of *causal flow* has been introduced: if the graph describing the entangled resource state has a causal flow then a deterministic MBQC can be driven on this resource. Causal flow has been generalized to a weaker condition called Generalized flow (Gflow) which is also sufficient for determinism. Gflow has been proved to be necessary for a robust variant of determinism and when roughly speaking there is no Pauli measurement, a special class of quantum measurements (see section 2 for details) [4]. In the same paper, the authors have introduced a weaker notion of flow called Pauli Flow, allowing some measurements to be Pauli measurements. Pauli flow is the weakest known sufficient condition for determinism and its necessity was a crucial open question as the characterisation of determinism in MBQC is the cornerstone of most of the applications of MBQC.

In section 2, we present the MBQC model, and the tools that come with it. Our first contribution is to provide a simpler characterisation of the Pauli flow (Proposition 1), with three instead of nine conditions to satisfy for the existence of a Pauli flow. Our main contribution is to prove in section 3 that the Pauli flow is not necessary in general – by pointing out several counter examples – but is actually necessary for *real* MBQC (Theorem 4). Real MBQC is a restriction of MBQC where only real observables are used, i.e. observables which eigenstates are quantum states that can be described using real numbers. Quantum mechanics, and hence models of quantum computation, are traditionally based on complex numbers. Real quantum computing is universal for quantum computation [1] and has been crucially used recently in the study of contextuality and simulation by means of quantum computing by state injection [9]. Real MBQC [14] may lead to several other applications. One of them is an interactive proof protocol built by McKague [12]. McKague introduced a protocol where a verifier using a polynomial number of quantum provers can perform a computation, with the guaranty that, if a prover has cheated, it will be able to detect it. An open question left in [12] by McKague is to know whether this model can bring to an interactive proof protocol with only two quantum provers. We answer negatively to this question in section 4.2. Our third contribution is to point out the existence of a kind of supernormal-form for Pauli flow in real MBQC on bipartite graphs (Lemma 6). This result enables us to prove in Theorem 5 that real MBQC on bipartite graphs is not very powerful: all measurements of a real bipartite MBQC can be parallelised. As a consequence, only problems that can be solved in constant depth can be solved using real bipartite MBQC.

2 Measurement-based quantum computation, Generalized Flow and Pauli Flow

Notations. We assume the reader familiar with quantum computing notations, otherwise one can refer to Appendix A or to [15]. We will use the following set/graph notations: First of all, the *symmetric difference* of two sets A and B will be denoted $A\Delta B := (A\cup B)\setminus(A\cap B)$. We will use intensively the *open* and *closed neighbourhood*. Given a simple undirected graph $G = (V, E)$, for any $u \in V$, $N(u) := \{v \in V \mid (u, v) \in E\}$ is the (open) neighbourhood of u, and $N[u] := N(u) \cup \{u\}$ is the closed neighbourhood of u. For any subset A of V, $\mathsf{Odd}(A) := \Delta_{v\in A}N(v)$ (resp. $\mathsf{Odd}[A] := \Delta_{v\in A}N[u]$) is the odd (resp. odd closed) neighbourhood of A. Also, we will use the notion of *extensive maps*. A map $f : A \to 2^B$, with $A \subseteq B$ is extensive if the transitive closure of $\{(u, v) : v \in f(u)\}$ is a strict partial order.

We say that f is extensive with respect to a strict partial order $\prec$ if $(v \in f(u) \Rightarrow u \prec v)$.

2.1 MBQC, concretely, abstractly

In this section, a brief description of the measurement-based quantum computation is given, a more detailed introduction can be found in [7, 8]. Starting from a low-level description of measurement-based quantum computation using the so-called patterns of the Measurement-Calculus – an assembly language composed of 4 kinds of commands: creation of ancillary qubits, entangling operation, measurement and correction – we end up with a graph theoretical description of the computation and in particular of the underlying entangled resource of the computation.

2.2 Measurement-Calculus patterns: an assembly language

An assembly language for MBQC is the Measurement-Calculus [7, 8]: a pattern is a sequence of commands, each command is either:
– N_u: initialisation of a fresh qubit u in the state $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$;
– $E_{u,v}$ entangling two qubits u and v by applying Control-Z operation $\Lambda Z : |x, y\rangle \mapsto (-1)^{xy} |x, y\rangle$ to the qubits u and v;
– $M_u^{\lambda_u,\alpha_u}$ measurement of qubit u according to the observable $\mathcal{O}_{\lambda_u,\alpha_u}$ described below;
– $X_u^{s_v}$ (resp. $Z_u^{s_v}$), a correction which consists of applying Pauli $X : |x\rangle \mapsto |1 - x\rangle$ (resp. $Z : |x\rangle \mapsto (-1)^x |x\rangle$) to qubit u iff s_v (the classical outcome of the measurement of qubit v) is 1.

A pattern is subject to some basic well-formedness conditions like: no operation can be applied on a qubit u after u being measured; a correction cannot depend on a signal s_u if qubit u is not yet measured.

The qubits which are not initialised using the N command are the input qubits, and those which are not measured are the output qubits. The measurement of a qubit u is characterized by $\lambda_u \subset \{X, Y, Z\}$ a subset of one or two Pauli operators, and an angle $\alpha_u \in [0, 2\pi)$:
– when $\lambda_u = \{M\}$ is a singleton, u is measured according to $\mathcal{O}_{\lambda_u,\alpha_u} := M$ if $\alpha_u = 0$ or $\mathcal{O}_{\lambda_u,\alpha_u} := -M$ if $\alpha_u = \pi$.
– when $|\lambda_u| = 2$, u is measured in the λ_u-plane of the Bloch sphere with an angle α_u, i.e. according to the observable:

$$\mathcal{O}_{\lambda_u,\alpha_u} := \begin{cases} \cos(\alpha_u)X_u + \sin(\alpha_u)Y_u & \text{if } \lambda_u = \{X, Y\} \\ \cos(\alpha_u)Y_u + \sin(\alpha_u)Z_u & \text{if } \lambda_u = \{Y, Z\} \\ \cos(\alpha_u)Z_u + \sin(\alpha_u)X_u & \text{if } \lambda_u = \{Z, X\} \end{cases}$$

Measurement of qubit u produces a classical outcome $(-1)^{s_u}$ where $s_u \in \{0, 1\}$ is called *signal*, or simply *classical outcome* with a slight abuse of notation.

2.3 A graph-based representation

In the Measurement-Calculus, the patterns are equipped with an equational theory which captures some basic invariant properties, e.g. two operations acting on distinct qubits commute, or $E_{u,v}$ is equivalent to $E_{v,u}$. It is easy to show using the equations of the Measurement-Calculus that any pattern can be transformed into an equivalent pattern of the form:

$$\left(\prod_{u\in O^c}^{\prec} Z_{\mathbf{z}(u)}^{s_u} X_{\mathbf{x}(u)}^{s_u} M_u^{\lambda_u,\alpha_u}\right)\left(\prod_{(u,v)\in G} E_{u,v}\right)\left(\prod_{u\in I^c} N_u\right)$$

where $G = (V, E)$ is a simple undirected graph, $I, O \subseteq V$ are respectively the input and output qubits, and $\mathtt{x}, \mathtt{z} : O^c \to 2^V$ are two extensive maps, i.e. the relation $\prec$ defined as the transitive closure of $\{(u, v) : v \in \mathtt{x}(u) \cup \mathtt{z}(u)\}$ is a strict partial order. Notice that $O^c := V \setminus O$ and $X^{s_u}_{\mathtt{x}(u)} := \prod_{v \in \mathtt{x}(u)} X^{s_u}_v$. Moreover the product $\prod_{(u,v)\in G}$ means that the indices are the edges of the G, in particular each edge is taken once.

The septuple $(G, I, O, \lambda, \alpha, \mathtt{x}, \mathtt{z})$ is a graph-based representation which captures entirely the semantics of the corresponding pattern. We simply call an MBQC such a septuple.

2.4 Semantics and Determinism

An MBQC $(G, I, O, \lambda, \alpha, \mathtt{x}, \mathtt{z})$ has a fundamentally probabilistic evolution with potentially $2^{|O^c|}$ possible branches as the computation consists of $|O^c|$ measurements. For any $s \in \{0,1\}^{|O^c|}$, let $A_s : \mathbb{C}^{\{0,1\}^I} \to \mathbb{C}^{\{0,1\}^O}$ be

$$A_s(|\varphi\rangle) = \left(\prod_{u \in O^c}^{\prec} Z^{s_u}_{\mathtt{z}(u)} X^{s_u}_{\mathtt{x}(u)} \left\langle \varphi^{\lambda_u,\alpha_u}_{s_u} \right|_u \right) \left(\prod_{(u,v)\in G} \Lambda Z_{u,v} \right) \left(|\varphi\rangle \otimes \frac{\sum_{x \in \{0,1\}^{I^c}} |x\rangle}{\sqrt{2^{|I^c|}}} \right)$$

where $\left|\varphi^{\lambda_u,\alpha_u}_{s_u}\right\rangle$ is the eigenvalue of $\mathcal{O}^{\lambda_u,\alpha_u}$ associated with the eigenvalue $(-1)^{s_u}$.

Given an initial state $|\varphi\rangle \in \mathbb{C}^{\{0,1\}^I}$ and $s \in \{0,1\}^{O^c}$, the outcome of the computation is the state $A_s |\Psi\rangle$ (up to a normalisation factor), with probability $\langle\varphi| A^\dagger_s A_s |\varphi\rangle$. In other words the MBQC implements the cptp-map[1] $\rho \mapsto \sum_{s \in \{0,1\}^{O^c}} A_s \rho A^\dagger_s$.

Among all the possible measurement-based quantum computations, those which are deterministic are of peculiar importance. In particular, deterministic MBQC are those which are used to simulate quantum circuits (cornerstone of the proof that MBQC is a universal model of quantum computation), or to implement a quantum algorithm. An MBQC $(G, I, O, \lambda, \alpha, \mathtt{x}, \mathtt{z})$ is **deterministic** if the output of the computation does not depend on the classical outcomes obtained during the computation: for any input state $|\varphi\rangle \in \mathbb{C}^{\{0,1\}^I}$ and branches $s, s' \in \{0,1\}^{O^c}$, $A_s |\varphi\rangle$ and $A_{s'} |\varphi\rangle$ are proportional.

Notice that the semantics of a deterministic MBQC $(G, I, O, \lambda, \alpha, \mathtt{x}, \mathtt{z})$ is entirely defined by a single branch, e.g. the branch $A_{0^{|O^c|}}$. Moreover, this particular branch $A_{0^{|O^c|}}$ is correction-free by construction (indeed all corrections are controlled by a signal, which is 0 in this particular branch). As a consequence, intuitively, when the evolution is deterministic, the corrections are only used to make the overall evolution deterministic but have no effect on the actual semantics of the evolution. Thus the correction can be abstracted away leading to the notion of **abstract MBQC** $(G, I, O, \lambda, \alpha)$. There is however a caveat when the branch $A_{0^{|O^c|}}$ is 0: for instance $M^{X,\pi}_1 N_1 N_2$ and $Z^{s_1}_2 M^{X,\pi}_1 N_1 N_2$ are both deterministic[2] and share the same abstract open graph, however they do not have the same semantics: the outcome of the former pattern is $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, whereas the outcome of the latter is $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

To avoid these pathological cases and guarantee that the corrections can be abstracted away, a stronger notion of determinism has been introduced in [4]: an MBQC is **strongly deterministic** when all the branches are not only proportional but equal up to a global phase. The strongness assumption guarantees that for any input state $|\varphi\rangle$, $A_{0^{|O^c|}} |\varphi\rangle$ is non zero, and thus guarantees that the overall evolution is entirely described by the correction-free branch, or in other words by the knowledge of the abstract MBQC $(G, I, O, \lambda, \alpha)$.

Whereas deterministic MBQC are not necessarily invertible (e.g. $M^{(X,0)}_1 N_2$ which maps any state $|\varphi\rangle$ to the state $|+\rangle$), strongly deterministic MBQC correspond to the invertible

[1] A completely positive trace-preserving map describes the evolution of a quantum system which state is represented by a density matrix. See for instance [15] for details.

[2] In both cases the unique measurement consists of measuring a qubit in state $|+\rangle$ according to the observable $-X$ which produces the signal $s_1 = 1$ with probability 1.

deterministic quantum evolutions: they implement isometries ($\exists U : \mathbb{C}^{\{0,1\}^I} \to \mathbb{C}^{\{0,1\}^O}$ s.t. $U^\dagger U = I$ and $\forall s \in \{0,1\}^{|O^c|}$, $\exists \theta$ s.t. $A_s = 2^{-|O^c|} e^{i\theta} U$).

We consider a variant of strong determinism which is robust to variation of the angles of measurements (which is a continuous parameter, so a priori subject to small variations in an experimental setting for instance), and to partial computation i.e., roughly speaking if one aborts the computation, the partial outcome does not depend on the branch of the computation.

Definition 1 (Robust Determinism)**.** $(G, I, O, \lambda, \alpha, \mathtt{x}, \mathtt{z})$ is robustly deterministic if for any lowerset $S \subseteq O^c$ and for any $\beta : S \to [0, 2\pi)$, $(G, I, O \cup S^c, \lambda|_S, \beta, \mathtt{x}|_S, \mathtt{z}|_S)$ is strongly deterministic, where S is a lowerset for the partial order induced by $\mathtt{x}$ and $\mathtt{z}$: $\forall v \in S, \forall u \in O^c$, $v \in \mathtt{x}(u) \cup \mathtt{z}(u) \Rightarrow u \in S$.

The notion of *robust determinism* we introduce is actually a short cut for *uniformly strong and stepwise determinism* which has been already extensively studied in the context of measurement-based quantum computing [4, 8, 13].

A central question in measurement-based quantum computation is to decide whether an abstract MBQC can be implemented deterministically: given $(G, I, O, \lambda, \alpha)$, does there exist correction strategies $\mathtt{x}, \mathtt{z}$ such that $(G, I, O, \lambda, \alpha, \mathtt{x}, \mathtt{z})$ is (robustly) deterministic? This question is related to the power of postselection in quantum computing: allowing postselection one can select the correction-free branch and thus implement any abstract MBQC $(G, I, O, \lambda, \alpha)$. Post-selection is a priori a non physical evolution, but in the presence of a correction strategy, postselection can be simulated using measurements and corrections.

The robustness assumption allows one to abstract away the angles and focus on the so-called **open graph** (G, I, O, λ) i.e. essentially the initial entanglement. For which initial entanglement – or in other words for which resource state – a deterministic evolution can be performed? This is a fundamental question about the structures and the computational power of entanglement.

Several graphical conditions for determinism have been introduced: causal flow, Generalized flow (Gflow) and Pauli Flow [6, 4, 8]. These are graphical conditions on open graphs which are sufficient to guarantee the existence of a robust deterministic evolution. Gflow has been proved to be a necessary condition for Pauli-free MBQC (i.e. for any open graph (G, I, O, λ) s.t. $\forall u \in O^c$, $|\lambda_u| = 2$). The necessity of Pauli flow was an open question[3]. In this paper we show that Pauli flow fails to be necessary in general, but is however necessary for real MBQC, i.e. when $\forall u \in O^c$, $\lambda_u \subseteq \{X, Z\}$. In the next section, we review the graphical sufficient conditions for determinism.

2.5 Graphical Conditions for Determinism

Several flow conditions for determinism have been introduced to guarantee robust determinism. Causal flow has been the first sufficient condition for determinism [6]. This condition has been extended to Generalized flow (Gflow) and Pauli flow [4]. Our first contribution is to provide a simpler description of the Pauli flow, equivalent to the original one (see appendix B):

Property 1. *(G, I, O, λ) has a Pauli flow iff there exist a strict partial order $<$ over O^c*

[3] In [4], an example of deterministic MBQC with no Pauli flow is given. This is however not a counter example to the necessity of the Pauli flow as the example is not robustly deterministic. More precisely not all the branches of computation occur with the same probability: with the notation of Figure 8 in [4] if measurements of qubits 4,6,8 produce the outcome 0, then the measurement of qubit 10 produces the outcome 0 with probability 1.

and $p : O^c \to 2^{I^c}$ *s.t.* $\forall u \in O^c$,

$$(c_X) \quad X \in \lambda_u \quad \Rightarrow \quad u \in \mathsf{Odd}(p(u)) \setminus \left(\bigcup_{\substack{v \geq u \\ v \notin O \cup \{u\}}} \mathsf{Odd}(p(v)) \right)$$

$$(c_Y) \quad Y \in \lambda_u \quad \Rightarrow \quad u \in \mathsf{Odd}[p(u)] \setminus \left(\bigcup_{\substack{v \geq u \\ v \notin O \cup \{u\}}} \mathsf{Odd}[p(v)] \right)$$

$$(c_Z) \quad Z \in \lambda_u \quad \Rightarrow \quad u \in p(u) \setminus \left(\bigcup_{\substack{v \geq u \\ v \notin O \cup \{u\}}} p(v) \right)$$

where $v \geq u$ *iff* $\neg(v < u)$

Remark. Notice that the existence of a Pauli flow forces the input qubits to be measured in the $\{X, Y\}$-plane: If (G, I, O, λ) has a Pauli flow then for any $u \in I \cap O^c$, $u \notin p(u)$ since $p(u) \subseteq I^c$. It implies, according to condition (c_Z), that $Z \notin \lambda_u$.

Gflow and Causal flows are special instances of Pauli flow: A Pauli flow is a Gflow when all measurements are performed in a plane (i.e. $\forall u$, $|\lambda_u| = 2$); a Causal flow [6] is nothing but a Gflow $(p, <)$ such that $\forall u, |p(u)| = 1$. GFlow has been proved to be a necessary and sufficient condition for robust determinism:

Theorem 2 ([4])**.** *Given an abstract MBQC* $(G, I, O, \lambda, \alpha)$ *such that* $\forall u \in O^c, |\lambda_u| = 2$*,* (G, I, O, λ) *has a GFlow* $(p, <)$ *if and only if there exists* $\mathtt{x}, \mathtt{z}$ *extensive with respect to* $<$ *s.t.* $(G, I, O, \lambda, \alpha, \mathtt{x}, \mathtt{z})$ *is robustly deterministic.*

Pauli flow is the most general known sufficient condition for determinism for robust determinism:

Theorem 3 ([4])**.** *If* (G, I, O, λ) *has a Pauli flow* $(p, <)$*, then for any* $\alpha : O^c \to [0, 2\pi)$*,* $(G, I, O, \lambda, \alpha, \mathtt{x}, \mathtt{z})$ *is robustly deterministic where* $\forall u \in O^c$*,*

$$\mathtt{x}(u) = \{v \in p(u) \mid u < v\}$$
$$\mathtt{z}(u) = \{v \in \mathsf{Odd}(p(u)) \mid u < v\}$$

Is there a converse? This is the purpose of next section.

3 Characterising Robust Determinism

In this section, we show the main result of the paper: Pauli flow is necessary for robust determinism in the real case, i.e. when all the measurements are in the $\{X, Z\}$-plane $(\forall u, \lambda_u \subseteq \{X, Z\})$.

We investigate in the subsequent sections the consequences of this result for real MBQC which is a universal model of quantum computation with several crucial applications.

A **real open graph** (G, I, O, λ) is an open graph such that $\forall u \in O^c, \lambda_u \subseteq \{X, Z\}$. We define similarly **real abstract MBQC** and **real MBQC**. Pauli flow conditions on real open graphs can be simplified as follows:

Property 2. *A real open graph (G, I, O, λ) has a Pauli flow iff there exist a strict partial order $<$ over O^c and $p : O^c \to 2^{I^c}$ s.t. $\forall u \in O^c$,*

$$(i) \quad X \in \lambda_u \quad \Rightarrow \quad u \in \mathsf{Odd}(p(u)) \setminus \left(\bigcup_{\substack{v \geq u \\ v \notin O \cup \{u\}}} \mathsf{Odd}(p(v)) \right)$$

$$(ii) \quad Z \in \lambda_u \quad \Rightarrow \quad u \in p(u) \setminus \left(\bigcup_{\substack{v \geq u \\ v \notin O \cup \{u\}}} p(v) \right)$$

Theorem 4. *Given a real abstract MBQC $(G, I, O, \lambda, \alpha)$, (G, I, O, λ) has a Pauli flow $(p, \prec)$ if and only if there exist $\mathtt{x}, \mathtt{z}$ extensive with respect to $\prec$ s.t. $(G, I, O, \lambda, \alpha, \mathtt{x}, \mathtt{z})$ is robustly deterministic.*

The proof of Theorem 4 is given in appendix. The proof is fundamentally different from the proof that Gflow is necessary for Pauli-free robust determinism (Theorem 2 in [4]). Roughly speaking, the proof that Pauli flow is necessary goes as follows: first we fix the inputs to be either $|0\rangle$ or $|+\rangle$ and all the measurements to be Pauli measurements (i.e. if $\lambda_u = \{X, Z\}$ we fix the measurement of u to be either X or Z). For each of these choices the computation can be described in the so-called stabilizer formalism which allows one to point out the constraints the corrections should satisfy for each of these particular choices of inputs and measurements. Then, as the corrections of a robust deterministic MBQC should not depend on the choice of the inputs and the angles of measurements, one can combine the constraints the corrections should satisfy and show that they coincide with the Pauli flow conditions.

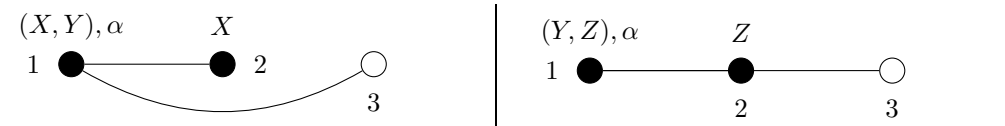
Remark. We consider in this paper a notion of real MBQC which corresponds to a constraint on the measurements ($\forall u \in O^c, \lambda_u \in \{X, Z\}$), it can also be understood as an additional constraint on the inputs: the input of the computation is in $\mathbb{R}^I$ instead of $\mathbb{C}^I$. This distinction might be important, for instance the pattern $M_1^Y N_2$ is strongly deterministic on real inputs but not on arbitrary complex inputs. It turns out that the proof of Theorem 4 only consider real inputs, and as a consequence is valid in both cases (i.e. when both inputs and measurements are real ; or when inputs are complex and measurements are in the $\{X, Z\}$-plane).

Pauli flow is necessary for real robust determinism. This property is specific to real measurements: Pauli flow is not necessary in general even when the measurements are restricted to one of the other two planes of measurements. In the following $\{X, Y\}$-MBQC (resp. $\{Y, Z\}$-MBQC) refers to MBQC where all measurements are performed in the $\{X, Y\}$-plane (resp. $\{Y, Z\}$-plane).

Property 3. *There exists robustly deterministic $\{X, Y\}$-MBQC (resp. $\{Y, Z\}$-MBQC) $(G, I, O, \lambda, \alpha, \mathtt{x}, \mathtt{z})$ such that (G, I, O, λ) has no Pauli flow $(p, \prec)$ where $\mathtt{x}$ and $\mathtt{z}$ are extensive with respect to $\prec$.*

Proof. We consider the pattern $\mathcal{P} = Z_3^{s_2} M_2^{X,0} X_2^{s_1} M_1^{\{X,Y\},\alpha} E_{1,2} E_{1,3} N_1 N_2 N_3$ which is an implementation of the $\{X, Y\}$-MBQC given in Fig 1 (the other example is similar). Notice that the correction $X_2^{s_1}$ is useless as qubit 2 is going to be measured according to M^X. Thus $\mathcal{P}$ has the same semantics as $\mathcal{P}' = Z_3^{s_2} M_2^{X,0} M_1^{\{X,Y\},\alpha} E_{1,2} E_{1,3} N_1 N_2 N_3$. Notice in $\mathcal{P}'$ that the two measurements commute since there is no dependency between them, leading to the pattern $\mathcal{P}'' = M_1^{\{X,Y\},\alpha} Z_3^{s_2} M_2^{X,0} E_{1,2} E_{1,3} N_1 N_2 N_3$. It is easy to check that $\mathcal{P}''$ has a Pauli flow so is robustly deterministic. All but the stepwise property are transported

by the transformations from $\mathcal{P}''$ to $\mathcal{P}$. Notice that $\mathcal{P}'$ is not stepwise deterministic as $M_1^{\{X,Y\},\alpha}E_{1,2}E_{1,3}N_1N_2N_3$ is not deterministic. However, $\mathcal{P}$ enjoys the stepwise property since $X_2^{s_1}M_1^{\{X,Y\},\alpha}E_{1,2}E_{1,3}N_1N_2N_3$ has a Pauli flow so is robustly deterministic. Finally, it is easy to show that the open graph has no Pauli flow $(p,\prec)$ such that $1 \prec 2$, which is necessary to guarantee that $\mathtt{x}$ is extensive with respect to $\prec$. □



$\mathtt{x}(1) = \{2\}$, $\mathtt{z}(1) = \emptyset$, $\mathtt{x}(2) = \emptyset$, $\mathtt{z}(2) = \{3\}$
$Z_3^{s_2}M_2^{X,0}X_2^{s_1}M_1^{\{X,Y\},\alpha}E_{1,2}E_{1,3}N_1N_2N_3$

$\mathtt{x}(1) = \emptyset$, $\mathtt{z}(1) = \{2\}$, $\mathtt{x}(2) = \emptyset$, $\mathtt{z}(2) = \{3\}$
$Z_3^{s_2}M_2^{Z,0}Z_2^{s_1}M_1^{\{Y,Z\},\alpha}E_{1,2}E_{2,3}N_1N_2N_3$

Figure 1: Robustly deterministic $\{X,Y\}$-MBQC and $\{Y,Z\}$-MBQC with no compatible Pauli flow. The two MBQC are described by means of there abstract MBQC (G,I,O,α) and the corrective maps $\mathtt{x}$ and $\mathtt{z}$. In both cases there is no input and the output is located on qubit 3. A description using the measurement-pattern formalism is also provided (commands should be read from right to left). Notice that the only order that makes $\mathtt{x}$ and $\mathtt{z}$ extensive has to verify $1 \prec 2$, and there is no Pauli flow for this order.

Remark. This is the last step of the proof of Theorem 4 which fails with the examples of Figure 1. For instance in the $\{X,Y\}$-MBQC example, in both cases of Pauli measurements of qubit 1 (according to X or according to Y), a Pauli flow exists, sharing the same partial order $1 \prec 2$. However the two Pauli flows are distinct and none of them is a Pauli flow when qubit 1 is measured in the $\{X,Y\}$-plane.

Remark. The examples given in figure 1 do have a Pauli flow but with a partial order not compatible with the order of measurements. It is important that the orders of the flow and the measurements coincide for guaranteeing that the depth of the flow (longest increasing sequence) corresponds to the depth of the MBQC. Because of the logarithmic separation between the quantum circuit model and MBQC in terms of depth (e.g. PARITY can be computed with a constant quantum depth MBQC but requires a logarithmic depth quantum circuit) [5], it is also important that Pauli flow characterises not only the ability to perform a robust deterministic evolution, but characterizes also the depth of such evolution. There exists an efficient polynomial time which, given an open graph, compute a Gflow of optimal depth (when it exists) [13], the existence of such an algorithm in the Pauli case is an open question.

4 Applications: Computational Power of Real Bipartite MBQC

In this section we focus on the real MBQC which underlying graph are bipartite (real bipartite MBQC for short). Bipartite graphs (or equivalently 2-colorable graphs) play an important role in MBQC, the square grid is universal for quantum computing: any quantum circuit can be simulated by an MBQC whose underlying graph is a square grid. The brickwork graph [2] is bipartite and universal for $\{X,Y\}$-MBQC. Regarding real MBQC, the (non bipartite) triangular grid is universal for real MBQC [14] but there is no known universal family of bipartite graphs. We show in this section that there is no universal family of bipartite graphs for real MBQC, by showing that any real bipartite MBQC can be done in constant depth.

4.1 Real bipartite MBQC in constant depth

In this section we show that real bipartite MBQC can always be parallelized:

Theorem 5. *All measurements of a robustly deterministic real bipartite MBQC can be performed in parallel.*

The rest of the section is dedicated to the proof of Theorem 5. According to Theorem 4, a real MBQC is robustly deterministic if and only if the underlying open graph has a Pauli flow. To prove that all the measurements can be performed in parallel in the bipartite case we point out the existence of a particular correction strategy which ensures that each measurement is corrected using output qubits only.

Lemma 6. *Given a bipartite graph G, $I, O \subseteq V(G)$ and $\lambda : O^c \to \{\{X\}, \{Z\}, \{X, Z\}\}$, if (G, I, O, λ) has a Pauli flow then there exists $p : O^c \to 2^{I^c}$ s.t.:*

$$\begin{aligned} \mathsf{Odd}(p(u)) \setminus (O \cup \lambda^{-1}(\{Z\})) &= \{u\} \setminus \lambda^{-1}(\{Z\}) \\ p(u) \setminus (O \cup \lambda^{-1}(\{X\})) &= \{u\} \setminus \lambda^{-1}(\{X\}) \end{aligned}$$

Proof. See appendix D □

This particular correction strategy corresponds to a king of *super-normal form*. Indeed it is known that Gflow can be put into the so called Z- or X-normal form but not both at the same time (see [10] for details). Lemma 6 shows, roughly speaking, that the Pauli flow in the real bipartite case can be put in both normal forms at the same time.

Proof of Theorem 5. Given a robustly deterministic real bipartite MBQC $(G, I, O, \lambda, \alpha, \mathtt{x}, \mathtt{z})$, according to Theorem 4, (G, I, O, λ) has a Pauli flow, so according to Lemma 6 there exists p s.t. $\mathsf{Odd}(p(u)) \setminus (O \cup \lambda^{-1}(\{Z\})) = \{u\} \setminus \lambda^{-1}(\{Z\})$ and $p(u) \setminus (O \cup \lambda^{-1}(\{X\})) = \{u\} \setminus \lambda^{-1}(\{X\})$. Notice that $(p, \emptyset)$ is a Pauli flow for (G, I, O, λ), thus according to Theorem 3, $(G, I, O, \lambda, \alpha, \mathtt{x}', \mathtt{z}')$ is robustly deterministic where $\mathtt{x}' = u \mapsto p(u) \setminus (\lambda^{-1}(\{X\}) \cup \{u\})$ and $\mathtt{z}' = u \mapsto \mathsf{Odd}(p(u)) \setminus (\lambda^{-1}(\{Z\}) \cup \{u\})$. Both $(G, I, O, \lambda, \alpha, \mathtt{x}, \mathtt{z})$ and $(G, I, O, \lambda, \alpha, \mathtt{x}', \mathtt{z}')$ implement the same computation, and $\forall u \in O^c$ $\mathtt{x}'(u) \subseteq O$ and $\mathtt{z}'(u) \subseteq O$ which implies that all measurements of the latter MBQC can be performed in parallel. □

4.2 Interactive proofs

The starting point of our work has been a sentence of McKague in [12]. In the future work section, McKague wonders how his work could be used to build an interactive prover with only two provers. The problem that McKaque wants to solve is the following. We imagine a classical verifier, which is a computer with classical resources, who wants to perform a computation using some non-communicating quantum provers. The quantum provers are computers with quantum resources. In fact, the classical verifier wants to achieve his computation using the quantum power of quantum provers. In this model, the hard point to breakthrough is that we want the verifier to detect cheating behavior of some provers. The model should guarantee the verifier that the result of the computation made by the provers is correct: if a prover has cheated and not computed what he was asked, the verifier should be able to detect it. We specify that the provers, in this model, cannot communicate one with the others: each prover can try to cheat on his own but he does not have the power to do it by exchanging information with the others. McKague, in [12], proves that it is possible to imagine a protocol in which the computation can be performed by the classical verifier using a polynomial number of quantum provers. To achieve this goal, McKague uses two main tools, one of them being Measurement Based Quantum Computation in the (X, Z) plane. Mhalla and Perdrix, in [14], prove that there exists a grid that enables to perform a universal computing in the (X, Z) plane. Usually, the (X, Y) plane, first known to allow

universal computation is preferred. In his work, McKague needs the (X, Z) plane: to be able to detect cheating behavior, McKague needs to compute in the reals. The conjugation operation that can be performed in other planes is a problem to detect some cheatings.

In his future work section, McKague argues that most his work could be used to improve his result to the use of only two provers. The main difficulty he points out is to build a bipartite graph to compute with. His self-testing skill, which is the second important tool of his work, can be applied only if the graph does not have any odd cycle. Therefore, the question we wanted to answer was whether one could build a universal bipartite grid for the (X, Z)-plane. Our Theorem 5 shows that in the real case a bipartite graph is not very powerful to compute: it is far from being universal. Therefore, at best, new skills will be needed to adapt McKague's method to interactive proofs with two provers.

5 Conclusion and future work

In this paper, we made substantial steps in understanding MBQC world. The first important one is this equivalence between being robustly deterministic and having a Pauli flow for a real-MBQC. Since it does not hold for $\{X, Y\}$- and $\{Y, Z\}$-planes, a natural question is how one can modify the Pauli flow definition to obtain a characterisation of determinism in these cases? A bi-product of the characterisation of robust determinism for real MBQC is the low comutational power of real bipartite MBQC. It would be interesting to compare the computational power of real bipartite MBQC and of commuting quantum circuits. There are some good reasons to think that the power of real bipartite MBQC is exactly the same as those commuting quantum circuits. Taking a global view of the MBQC domain, some advances we make in this paper, and a good direction for further research should be to better understand the specificity of each plane in the power of the MBQC model and how the ability to perform a deterministic computation is linked to this power. Finally, another open question is the existence of an efficient algorithm for deciding whether a given open graph has a Pauli flow, and which produces a Pauli flow of optimal depth when it exists. Such an algorithm exists for Gflow [13].

References

[1] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM J. Comput.*, 26:1411–1478, 1997.

[2] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *50th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2009*, 2009. URL: *http://www.citebase.org/abstract?id = oai:arXiv.org:*0807.4154.

[3] Anne Broadbent and Elham Kashefi. Parallelizing quantum circuits. *Theoretical Computer Science*, 410(26):2489–2510, 2009.

[4] Daniel E. Browne, Elham Kashefi, Mehdi Mhalla, and Simon Perdrix. Generalized flow and determinism in measurement-based quantum computation. *New Journal of Physics (NJP)*, 9(8), 2007. URL: *http://iopscience.iop.org/*1367 − 2630/9/8/250/*fulltext/*.

[5] Daniel E. Browne, Elham Kashefi, and Simon Perdrix. Computational depth complexity of measurement-based quantum computation. In *Theory of Quantum Computation, Communication, and Cryptography (TQC'10)*, volume 6519, pages 35–46. LNCS, 2011.

[6] Vincent Danos and Elham Kashefi. Determinism in the one-way model. *Physical Review A*, 74(052310), 2006.

[7] Vincent Danos, Elham Kashefi, and Prakash Panangaden. The measurement calculus. *J. ACM*, 54(2), 2007.

[8] Vincent Danos, Elham Kashefi, Prakash Panangaden, and Simon Perdrix. *Extended Measurement Calculus*. Cambridge University Press, 2010.

[9] Nicolas Delfosse, Philippe Allard Guerin, Jacob Bian, and Robert Raussendorf. Wigner function negativity and contextuality in quantum computation on rebits. *Physical Review X*, 5(2):021003, 2015.

[10] Nidhal Hamrit and Simon Perdrix. *Reversibility in Extended Measurement-Based Quantum Computation*, pages 129–138. Springer International Publishing, Cham, 2015.

[11] M. Hein, J. Eisert, and H. J. Briegel. Multi-party entanglement in graph states. *Physical Review A*, 69:062311, 2004. URL: *doi*:10.1103/*PhysRevA*.69.062311.

[12] Matthew McKague. Interactive proofs for bqp via self-tested graph states. *Theory of Computing*, 12(3):1–42, 2016.

[13] Mehdi Mhalla and Simon Perdrix. Finding optimal flows efficiently. In *the 35th International Colloquium on Automata, Languages and Programming (ICALP), LNCS*, volume 5125, pages 857–868, 2008.

[14] Mehdi Mhalla and Simon Perdrix. Graph States, Pivot Minor, and Universality of (X, Z)-Measurements. *International Journal of Unconventional Computing*, 9(1-2):153–171, 2013.

[15] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, New York, NY, USA, 2000.

[16] Robert Prevedel, Philip Walther, Felix Tiefenbacher, Pascal Bohi, Rainer Kaltenbaek, Thomas Jennewein, and Anton Zeilinger. High-speed linear optics quantum computing using active feed-forward. *Nature*, 445(7123):65–69, January 2007. URL: *http://dx.doi.org/*10.1038/*nature*05346, *http://dx.doi.org/*10.1038/*nature*05346 *doi*:10.1038/*nature*05346.

[17] Robert Raussendorf. Contextuality in measurement-based quantum computation. *Physical Review A*, 88(2):022322, 2013.

[18] Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188–5191, 2001.

[19] Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel. Measurement-based quantum computation with cluster states. *Physical Review A*, 68:022312, 2003. URL: *http://arxiv.org/abs/quant − ph/*0301052.

[20] Robert Raussendorf, Jim Harrington, and Kovid Goyal. A fault-tolerant one-way quantum computer. *Annals of physics*, 321(9):2242–2270, 2006.

[21] Philip Walther, Kevin J. Resch, Terry Rudolph, Emmanuel Schenck, Harald Weinfurter, Vlatko Vedral, Markus Aspelmeyer, and Anton Zeilinger. Experimental one-way quantum computing. *Nature*, 434(7030):169–176, March 2005. URL: *http://dx.doi.org/*10.1038/*nature*03347, *http://dx.doi.org/*10.1038/*nature*03347 *doi*:10.1038/*nature*03347.

A Quantum Computing in a Nutshell

The state of a given a finite set (or register) A of qubits is a unit vector $|\varphi\rangle \in \mathbb{C}^{\{0,1\}^A}$. The so-called classical states $\{|x\rangle : x \in \{0,1\}^A\}$ of the register A form an orthonormal basis $\mathbb{C}^{\{0,1\}^A}$, thus any state $|\varphi\rangle$ of A can be described as $|\varphi\rangle = \sum_{x\in\{0,1\}^A} \alpha_x |x\rangle$ s.t. $\sum_{x\in\{0,1\}^A} |\alpha_x|^2 = 1$. Given two distinct registers A and B, if the state of A is $|\varphi\rangle = \sum_{x\in\{0,1\}^A} \alpha_x |x\rangle$ and the state of B is $|\psi\rangle = \sum_{y\in\{0,1\}^B} \beta_y |y\rangle$, then the state of the overall register $A \cup B$ is $|\varphi\rangle \otimes |\psi\rangle = \sum_{x\in\{0,1\}^A, y\in\{0,1\}^B} \alpha_x\beta_y |xy\rangle$, where xy is the concatenation of x and y.

The adjoint of a state $|\varphi\rangle = \sum_{x\in\{0,1\}^A} \alpha_x |x\rangle \in \mathbb{C}^{\{0,1\}^A}$ is $\langle\varphi| = (|\varphi\rangle)^\dagger = \sum_{x\in\{0,1\}^A} \alpha_x^* \langle x| \in \mathbb{C}^{\{0,1\}^A} \to 1$, where $\forall x, y \in \{0,1\}^A$, $\langle x|\, |y\rangle = \delta_{x,y}$.

Any quantum evolution can be decomposed into a sequence of *isometries* and *measurements*: An isometry $U : \mathbb{C}^{\{0,1\}^A} \to \mathbb{C}^{\{0,1\}^B}$ is a linear map s.t. $U^\dagger U = I$, (i.e. $\forall x \in \{0,1\}^A, (U|x\rangle)^\dagger (U|x\rangle) = 1$), which transforms the state $|\varphi\rangle$ into $U|\varphi\rangle$. Famous examples of isometries are the unitary evolutions which correspond to the case $|A| = |B|$. The simplest example of unitary transformations are the so-called one-qubit Pauli operators X, Y, Z: $X = |x\rangle \mapsto |1-x\rangle$, $Z = |x\rangle \mapsto (-1)^x |x\rangle$ and $Y = iXZ$. An example of an isometry which is not a unitary evolution is, given a one-qubit state $|\psi\rangle \in \{0,1\}^{\{u\}}$ and a register A s.t. $u \notin A$, the map $|\psi\rangle_u : \mathbb{C}^{\{0,1\}^A} \to \mathbb{C}^{\{0,1\}^{A\cup\{u\}}} = |\varphi\rangle \mapsto |\varphi\rangle \otimes |\psi\rangle$ which consists of adding a qubit u in the state $|\psi\rangle$ to the register A.

A measurement is a fundamentally probabilistic evolution which produces a classical outcome and transforms the state of the quantum system. We consider in this paper only destructive measurements which means that the measured qubit is consumed by the measurement: measuring a qubit u of a register A transforms the state $|\varphi\rangle \in \{0,1\}^A$ into a state $|\psi\rangle \in \{0,1\}^{A\setminus\{u\}}$. Moreover, we will consider only one-qubit measurements, also called local measurements. A 1-qubit measurement is characterised by an observable $\mathcal{O}$, i.e. an hermitian operator acting on one qubit. We assume $\mathcal{O}$ has two distinct eigenvalues 1 and -1. Let $|\varphi_0\rangle$ and $|\varphi_1\rangle$ be the corresponding eigenvectors. A measurement according to $\mathcal{O}$ of a qubit u of a register A in the state $|\psi\rangle \in \mathbb{C}^{\{0,1\}^A}$ produces the classical outcome 0 (resp. 1) and the state $\frac{\langle\varphi_0|_u|\psi\rangle}{\sqrt{\langle\varphi||\varphi_0\rangle_u\langle\varphi_0|_u|\psi\rangle}}$ (resp. $\frac{\langle\varphi_1|_u|\psi\rangle}{\sqrt{\langle\varphi||\varphi_1\rangle_u\langle\varphi_0|_u|\psi\rangle}}$) with probability $\langle\varphi|\,|\varphi_0\rangle_u\langle\varphi_0|_u|\psi\rangle$ (resp. $\langle\varphi|\,|\varphi_1\rangle_u\langle\varphi_1|_u|\psi\rangle$), where $\langle\varphi_1|_u : \mathbb{C}^{\{0,1\}^{A\cup\{u\}}} \to \mathbb{C}^{\{0,1\}^A}$ is the adjoint of $|\varphi_1\rangle_u$.

A quantum evolution composed of k 1-qubit measurements and n isometries (in any order) has 2^k possible evolutions and is hence represented by 2^k linear maps L_s indexed by the possible sequences of classical outcomes. The quantum evolution should satisfy the condition $\sum_{s\in\{0,1\}^k} L_s^\dagger L_s = I$. It can be obtained as the composition of isometries and measurements as follows: a measurement is a pair $\{\langle\varphi_0|, \langle\varphi_1|\}$, an isometry U is a singleton $\{U\}$ and the composition of two quantum evolutions is $\{L_s : s \in \{0,1\}^k\} \circ \{M_t : t \in \{0,1\}^m\} = \{L_sM_t : s \in \{0,1\}^k, t \in \{0,1\}^m\}$.

A probability distribution of quantum states, say $\{(|\varphi_i\rangle, p_i)\}_i$ can be represented as a density matrix $\rho = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|$. Two probability distributions of quantum states leading to the same density matrix are indistinguishable. A quantum evolution $\{L_s : s \in \{0,1\}^k\}$ transforms ρ into $\sum_{s\in\{0,1\}^k} L_s\rho L_s^\dagger$.

B Proof of property 1

Pauli flow has been introduced in [4], as follows:

Definition 7 (Pauli Flow [4])**.** An open graph state (G, I, O, λ) has *Pauli flow* if there exists a map $p : O^c \to 2^{I^c}$ and a strict partial order $<$ over O^c such that $\forall u, v \in O^c$,
—(P1) if $v \in p(u)$, $u \neq v$, and $\lambda_v \notin \{\{X\}, \{Y\}\}$ then $u < v$,
—(P2) if $v \leq u$, $u \neq v$, and $\lambda_v \notin \{\{Y\}, \{Z\}\}$ then $v \notin \mathsf{Odd}(p(u))$,

—(P3) if $v \leq u$, $u \neq v$, and $\lambda_v = \{Y\}$ then $v \in p(u) \Leftrightarrow v \in \mathsf{Odd}(p(u))$,
—(P4) if $\lambda_u = \{X, Y\}$ then $u \notin p(u)$ and $u \in \mathsf{Odd}(p(u))$,
—(P5) if $\lambda_u = \{X, Z\}$ then $u \in p(u)$ and $u \in \mathsf{Odd}(p(u))$,
—(P6) if $\lambda_u = \{Y, Z\}$ then $u \in p(u)$ and $u \notin \mathsf{Odd}(p(u))$,
—(P7) if $\lambda_u = \{X\}$ then $u \in \mathsf{Odd}(p(u))$,
—(P8) if $\lambda_u = \{Z\}$ then $u \in p(u)$,
—(P9) if $\lambda_u = \{Y\}$ then either: $u \notin p(u)$ & $u \in \mathsf{Odd}(p(u))$ or $u \in p(u)$ & $u \notin \mathsf{Odd}(p(u))$.
where $u \leq v$ iff $\neg(v < u)$.

First of all, (P9) can be simplified to: if $\lambda_u = \{Y\}$ then $u \in \mathsf{Odd}[p(u)]$. Let's now begin to rewrite the block (P4) to (P9). Using (P4), (P5) and (P7), we can say that $X \in \lambda_u \Rightarrow u \in \mathsf{Odd}(p(u)$. Also, (P4), (P6) and (P9) enable us to show that $Y \in \lambda_u \Rightarrow u \in \mathsf{Odd}[p(u)]$ and (P5), (P6) and (P8) that $Z \in \lambda_u \Rightarrow u \in p(u)$ is correct. Conversely, we can go back as easily to property (P4) to (P9) from $X \in \lambda_u \Rightarrow u \in \mathsf{Odd}(p(u))$, $Y \in \lambda_u \Rightarrow u \in \mathsf{Odd}[p(u)]$ and $Z \in \lambda_u \Rightarrow u \in p(u)$.

To achieve the proof, we need to show that given a $u \in O^c$, for all $v \in O^c$, (P1), (P2) and (P3) are equivalent to the fact that if $v \leq u$ and $v \neq u$, then:
—(Q1) $X \in \lambda_v \Rightarrow v \notin \mathsf{Odd}(p(u))$,
—(Q2) $Y \in \lambda_v \Rightarrow v \notin \mathsf{Odd}[p(u)]$,
—(Q3) $Z \in \lambda_v \Rightarrow v \notin p(u)$.

This equivalence is easier to prove once (P1), (P2) and (P3) are simplified to:
—(P1') for $v \leq u$ and $v \neq u$, $\lambda_v \notin \{\{X\}, \{Y\}\} \Rightarrow v \notin p(u)$,
—(P2') for $v \leq u$ and $v \neq u$, $\lambda_v \notin \{\{Y\}, \{Z\}\} \Rightarrow v \notin \mathsf{Odd}(p(u))$,
—(P3') for $v \leq u$ and $v \neq u$, $\lambda_v = \{Y\}$, $v \in p(u) \Leftrightarrow v \in \mathsf{Odd}(p(u))$.

The end of the proof is a proof by exhaustion. To prove (Q1) from (P1'), (P2') and (P3'), let's say that if $X \in \lambda_v$, then λ_v is $\{X\}$, $\{X, Y\}$ or $\{X, Z\}$. (P2') enables us to conclude. To prove (Q2), let's say that if $Y \in \lambda_v$, then λ_v is $\{Y\}$, $\{X, Y\}$ or $\{Y, Z\}$. In the first case, we can conclude from (P3'), in the other two, the combination of (P1') and (P2') do the trick. The third case goes the same way.

Conversely, let's show that we can prove (P1') from (Q1), (Q2) and (Q3). The proof of (P2') and (P3') will follow the same sketch. If $\lambda_v \notin \{\{X\}, \{Y\}\}$, then λ_v is $\{Z\}$ or one of the three planes. If λ_v is $\{Z\}$, $\{X, Z\}$ or $\{Y, Z\}$, then we get the result from (Q3). If λ_v is $\{X, Y\}$, then we know from (Q1) that $v \notin \mathsf{Odd}[p(u)]$ and from (Q2) that $v \notin \mathsf{Odd}(p(u))$: that sufficient to assure that $v \notin p(u)$. That ends the proof.

C Proof of Theorem 4

[$\Rightarrow$]: Theorem 3. [$\Leftarrow$]: We order the vertices of G according to the order of the measurements: $V = \{v_0, \ldots, v_{n-1}\}$ s.t. $v_i \prec v_j \Rightarrow i < j$. For any $k \in [0, n)$, let $V_k = \{v_k, \ldots, v_{n-1}\}$. For any $S \subseteq I$, let the input in S be $|0\rangle$ and those in $I \setminus S$ be $|+\rangle$. Moreover for any $u \in O^c$, let M_u be a Pauli measurement of qubit u with $M \in \lambda_u$. The initial state – before the first measurement – is $|\varphi_0\rangle = |0\rangle_S \otimes (\prod_{u,v \in S^c s.t.(u,v) \in G} \Lambda Z_{u,v}) |+\rangle_{S^c}$. We are going to use some technical claims to build the proof, for which the proofs are given in appendix C. The following claims exhibit Pauli operators which depend on the measurements performed during the computation, and which stabilize the intermediate states obtained during the computation:

Claim 1. There exists n independent[4] Pauli operators $P^{(0)}, \ldots, P^{(n-1)} : \mathbb{C}^{\{0,1\}^V} \to \mathbb{C}^{\{0,1\}^V}$ s.t. $\forall i \in [0, n)$, $P^{(i)} |\varphi_0\rangle = |\varphi_0\rangle$ and $\forall j < i$, M_{v_j} and $P^{(i)}$ commute.

[4] $P^{(0)}, \ldots, P^{(n-1)}$ are independent if none of these Pauli operators can be obtained as the product of the other ones, even up to a global phase.

[Proof of Claim 1] For all $u \in V$, let $R^{(u)} = \begin{cases} Z_u & \text{if } u \in S \\ X_u Z_{N_G(u)} & \text{otherwise} \end{cases}$. The initial state $|\varphi_0\rangle$ is stabilized by $\mathcal{S} = \langle R_u \rangle_{u \in V}$, i.e. $|\varphi_0\rangle$ is the unique state (up to an irrelevant global phase) such that $\forall u \in V(G)$, $R_u |\varphi_0\rangle = |\varphi_0\rangle$.

We use the following Gauss-elimination-like algorithm to produce some new generators $(P^{(u)})_{u \in V}$ of $\mathcal{S}$ which satisfy that $\forall v_i \in O^c, \forall v_j \in V$, if $i < j$ then M_{v_i} and $P^{(v_j)}$ commute:

For all $u \in V, P^{(u)} \leftarrow R^{(u)}$.
For all $i \in [0, |V| - 1]$:
  let $A = \{j \mid i \leq j$ and M_{v_i} and $P^{(v_j)}$ anticommute$\}$.
  If $A \neq \emptyset$, let $i_0 \in A$
    for all $j \in A \setminus \{i_0\}$, $P^{(v_j)} \leftarrow P^{(v_j)}.P^{(v_{i_0})}$
    $P_{v_i} \leftrightarrow P_{v_{i_0}}$. □

Claim 2. After k measurements and the corresponding corrections, the state $|\varphi_k\rangle$ of the system[5] satisfies: $\forall i < k$, $M_{v_i} |\varphi_k\rangle = \pm |\varphi_k\rangle$ and $\forall i \geq k$, $P^{(i)} |\varphi_k\rangle = |\varphi_k\rangle$.

[Proof of Claim 2.] Since the first k qubits of $|\varphi_k\rangle$ have been measured according to $M_{v_0}, ..., M_{v_{k-1}}$, for any $i < k$, $M_{v_i} |\varphi_k\rangle = (-1)^{s_i} |\varphi_k\rangle$ where $s_i \in \{0, 1\}$ is the classical outcome of measurement of qubit v_i. To prove that $\forall i \geq k$, $P^{(i)} |\varphi_k\rangle = |\varphi_k\rangle$, notice that if a quantum state is the fixpoint of some operator P, the measurement of this state according to an observable which commute with P produces, whatever the classical outcome is, a quantum state which is also a fixpoint of P. Thus, since $P^{(i)}$ stabilizes the initial state $|\varphi_0\rangle$ and commutes with the first k measurements, it stabilizes $|\varphi_k\rangle$. □

Claim 3. For any k, and any n-qubit Pauli operator P s.t. $P |\varphi_k\rangle = \pm |\varphi_k\rangle$, $\exists B_S \subseteq S^c$, $\exists D_S \subseteq S$, $\exists F_S \subseteq V_k^c$ s.t. $P = \pm X_{B_S} Z_{\mathsf{Odd}(B_S) \Delta D_S} \prod_{u \in F_S} M_u$.

[Proof of Claim 3.] Claim 2 provides n independent Pauli operators which stabilize $|\varphi_k\rangle$ thus P must be a product of these operators: $\exists F_S \subseteq V_k^c$, $\exists Q \subseteq [k, n)$, s.t. $P = \pm \prod_{u \in F_S} M_u \prod_{i \in Q_S} P^{(i)}$. Since each $P^{(i)}$ is, according to Claim 1, a product $\prod_{u \in \Gamma_i} R_u$ where of $R_u = \begin{cases} Z_u & \text{if } u \in S \\ X_u Z_{N_G(u)} & \text{otherwise} \end{cases}$. As a consequence, $P = \pm X_{B_S} Z_{\mathsf{Odd}(B_S) \Delta D_S} \prod_{u \in F_S} M_u$, where $D_S = (\Gamma_k \Delta \dots \Delta \Gamma_{n-1}) \cap S$ and $B_S = (\Gamma_k \Delta \dots \Delta \Gamma_{n-1}) \cap S^c$. □

At some step k of the computation, by the strongness hypothesis, the two possible outcomes of the measurement according to M_{v_k} occur with probability 1/2. Thus, thanks to the stepwise determinism hypothesis, there exists a real state $|\psi\rangle$ on qubits $V \setminus \{v_k\}$ and $\theta \in [0, 2\pi)$ s.t.

$$|\varphi_k\rangle = \frac{1}{\sqrt{2}} (|\uparrow\rangle_{v_k} \otimes |\varphi\rangle_{V \setminus \{v_k\}} + e^{i\theta} |\downarrow\rangle_{v_k} \otimes X_{\mathbf{x}(v_k)} Z_{\mathbf{z}(v_k)} |\varphi\rangle_{V \setminus \{v_k\}})$$

where $|\uparrow\rangle \in \{|0\rangle, \frac{|0\rangle + |1\rangle}{\sqrt{2}}\}$ and $|\downarrow\rangle \in \{|1\rangle, \frac{|0\rangle - |1\rangle}{\sqrt{2}}\}$ are the eigenvectors of M_{v_k}. Since $|\varphi_k\rangle$, $|\uparrow\rangle$, $|\downarrow\rangle$ and $|\varphi\rangle$ are real states, $e^{i\theta} = (-1)^r$ for some $r \in \{0, 1\}$. Let T be the Pauli operator s.t. $T |\uparrow\rangle = - |\downarrow\rangle$ and $T |\downarrow\rangle = (-1)^{|\mathbf{x}(v_{k+1}) \cap \mathbf{z}(v_{k+1})|} |\uparrow\rangle$.

Since $(-1)^r M_{v_k} T_{v_k} X_{\mathbf{x}(v_k)} Z_{\mathbf{z}(v_k)} |\varphi_k\rangle = |\varphi_k\rangle$, according to claim 3, $\exists B_S \subseteq S^c, D_S \subseteq S, F_S \subseteq V_k^c$ s.t. $M_{v_k} T_{v_k} X_{\mathbf{x}(v_k)} Z_{\mathbf{z}(v_k)} = \pm X_{B_S} Z_{Odd(B_S) \Delta D_S} \prod_{u \in F_S} M_u$. Thus,

[5] To simplify the proof we assume that the measurements are non destructive, which means that after, say, a Z-measurement the measured qubit remains and is either in state $|0\rangle$ of $|1\rangle$ depending on the outcome of the measurement. As a consequence, for any k, $|\varphi_k\rangle$ is a n-qubit state.

$$T_{v_k} X_{\mathbf{x}(v_k)} Z_{\mathbf{z}(v_k)} = \pm X_{B_S} Z_{Odd(B_S)\Delta D_S} \prod_{u \in F'_S} M_u$$

with $B_S \subseteq S^c, D_S \subseteq S, F'_S \subseteq V^c_{k+1}$.

The equation above, involving $\mathbf{x}(v_k)$ and $\mathbf{z}(v_k)$, is the main ingredient to recover the Pauli flow conditions. However, this equation depends a priori on the choice of the measurements and the initial sates. The following claims, proved in appendix, show how to get rid of this dependency.

Claim 4. B_S, D_S, and F'_S do not depend on S. Therefore, using the notation F, B and D respectively, we can notice that $D = D_\emptyset = \emptyset$, and $B = B_I \subseteq I^c$.

[**Proof of Claim 4.**] For any $S, S' \subseteq I$,
$X_{B_S \Delta B_{S'}} Z_{Odd(B_S \Delta B_{S'})\Delta D_S \Delta D_{S'}} \prod_{u \in F'_S \Delta F'_{S'}} M_u = \pm I$, so $\prod_{u \in F'_S \Delta F'_{S'}} M_u = \pm X_{B_S \Delta B_{S'}} Z_{Odd(B_S \Delta B_{S'})\Delta D_S \Delta D_{S'}}$.
Since all $M_u \in \{X, Z\}$, the product in the RHS of the latter equation should only produce X and Z (but no XZ), thus $(B_S \Delta B_{S'}) \cap (Odd(B_S \Delta B_{S'}) \Delta D_S \Delta D_{S'}) = \emptyset$ which is equivalent to $(B_S \Delta B_{S'}) \cap (D_S \Delta D_{S'}) = (B_S \Delta B_{S'}) \cap (Odd(B_S \Delta B_{S'}))$. Thus $|(B_S \Delta B_{S'}) \cap (D_S \Delta D_{S'})| = 0 \bmod 2$, since for any set A, $|A \cap Odd(A)| = 0 \bmod 2$.

To prove that $F'_S = F'_{S'}$ we exhibit a particular input state such that the initial state is an eigenvector of $\prod_{u \in F'_S \Delta F'_{S'}} M_u$. It implies that when the measurements are performed, the last measurement of $F'_S \Delta F'_{S'}$ is going to be deterministic and thus contradicts the strongness assumption. As a consequence $F'_S \Delta F'_{S'}$ must be empty. The input state is constructed as follows: The qubits in $(B_S \Delta B_{S'}) \cap I$ are initialised in $|+\rangle$, the others in $|0\rangle$. Since $|(B_S \Delta B_{S'}) \cap (D_S \Delta D_{S'})| = 0 \bmod 2$ there exists a partition of $(B_S \Delta B_{S'}) \cap (D_S \Delta D_{S'})$ into pairs of qubits $P = \{(u_i, v_i)\}_i$. For each pair in P, ΛZ is applied on the corresponding qubits. The input state is then a fixpoint of $X_{(B_S \Delta B_{S'}) \cap I} Z_{D_S \Delta D_{S'}}$, thus after the entangling stage the overall state (including input and non input qubits) is an eigenstate of $X_{B_S \Delta B_{S'}} Z_{Odd(B_S \Delta B_{S'}) \Delta D_S \Delta D_{S'}}$ which implies that the measurement according to $\prod_{u \in F'_S \Delta F'_{S'}} M_u$ is not strong. As a consequence, $F_S = F_{S'}$ which implies $B_S = B_{S'}$ and $D_S = D_{S'}$. □

Claim 5. F and B do not depend on the choice of Pauli measurements.

[**Proof of Claim 5.**] If F and B depend on the choice of the Pauli measurements then there exists two choices which differ on a single measurement and differ on at least one of the sets F, B. Let $(M_u)_{u \in O^c}$ and $(M'_u)_{u \in O^c}$ these two choices and $u_0 \in O^c$ s.t. $\forall u \neq u_0$, $M_u = M'_u$ and $M_{u_0} \neq M'_{u_0}$. Let B, F and B', F' the sets associated with these two choices of measurements. We have $X_{B \Delta B'} Z_{Odd(B \Delta B')} = \prod_{u \in F \setminus F'} M_u \prod_{u \in F' \setminus F} M'_u \prod_{u \in F \cap F'} M_u M'_u$. Notice that $\prod_{u \in F \cap F'} M_u M'_u = \begin{cases} I & \text{if } u_0 \notin F \cap F' \\ X_{u_0} Z_{u_0} & \text{if } u_0 \in F \cap F' \end{cases}$. Since $|(B \Delta B') \cap Odd(B \Delta B')| = 0 \bmod 2$, we know that $\prod_{u \in F \cap F'} M_u M'_u = I$.
As a consequence, $X_{B \Delta B'} Z_{Odd(B \Delta B')} = \prod_{u \in F \Delta F'} M_u$. Using similar arguments that has been used above, one can provide a particular input such that the state is a fixpoint of $\prod_{u \in F \Delta F'} M_u$ which implies that, if $F \Delta F' \neq \emptyset$ the last measurement of $F \Delta F'$ is deterministic, contradicting the strongness hypothesis. Thus $F = F'$, as a consequence $B = B'$. □

We are now able to build a Pauli flow. Since F does not depend on the choice of the measurements, the basis of measurement of the qubits in F must not vary, i.e. $F \subseteq \lambda^{-1}(\{X\}) \cup \lambda^{-1}(\{Z\})$. As a consequence, defining $F_X = F \cap \lambda^{-1}(\{X\}))$ and $F_Z = F \cap \lambda^{-1}(\{Z\}))$, we have $T_{v_k} X_{\mathbf{x}(v_k)} Z_{\mathbf{z}(v_k)} = \pm X_{B \Delta F_X} Z_{Odd(B) \Delta F_Z}$. Defining $p(v_k) := B$ one can double check that for any partial order $\prec$ with respect to which $\mathbf{x}$ and $\mathbf{z}$ are extensive, $(p, \prec)$

is a Pauli flow. Indeed, if $X \in \lambda_{v_k}$, T anti-commutes with X, thus $u \in Odd(p(v_k))$. Similarly if $Z \in \lambda_u$, $u \in p(v_k)$.

Let $u \leq v_k$, $u \neq v_k$. Since $\mathtt{x}$ and $\mathtt{z}$ are extensive, it implies that $u \notin \mathtt{x}(v_k) \cup \mathtt{z}(v_k)$. If $u \in Odd(p(v_k))$, $u \in F_Z$ so $u \in \lambda^{-1}(\{Z\})$ which implies that $X \notin \lambda_u$. So $X \in \lambda_u \Rightarrow u \notin Odd(p(v_k))$. Similarly $Z \in \lambda_u \Rightarrow u \notin p(v_k)$ □

D Proof of Lemma 6

Since (G, I, O, λ) has a Pauli flow, there exists an order $<$ and $g : O^c \to 2^{I^c}$ s.t. $X \in \lambda_u \Rightarrow u \in \mathsf{Odd}(g(u)) \setminus \left(\bigcup_{\substack{v \geq u \\ v \neq u}} \mathsf{Odd}(g(v)) \right)$ and $Z \in \lambda_u \Rightarrow u \in g(u) \setminus \left(\bigcup_{\substack{v \geq u \\ v \neq u}} g(v) \right)$. Since G is bipartite, let V_0, V_1 be a bipartition of $V(G)$ s.t. V_0 and V_1 are independent sets, and let $R_i = V_i \setminus O$ and $p : O^c \to 2^{I^c}$ be defined as follows: $\forall i \in \{0,1\}$, and $\forall u \in R_i$,

$$p(u) := g(u) \oplus \left(\bigoplus_{\substack{v \in \mathsf{Odd}(g(u)) \setminus \{u\} \\ \text{s.t.} X \in \lambda_v}} p_Z(v) \right) \oplus \left(\bigoplus_{\substack{v \in g(u) \setminus \{u\} \\ \text{s.t.} Z \in \lambda_v}} p_X(v) \right)$$

where $\forall i \in \{0,1\} \forall v \in R_i$, $p_X(v) = p(v) \cap V_i$, and $p_Z(v) = p(v) \cap V_{1-i}$.

The inductive definition of p is well founded as the definition of $p(u)$ only depends on $p(v)$ with $u < v$.

Let u be maximal for $<$, $\mathsf{Odd}(p(u)) = \mathsf{Odd}(g(u))$. For any $v < u$, $v \in (O \cup \lambda^{-1}(\{Z\}))^c$ implies $X \in \lambda_v$, so according to the Pauli flow condition, $v \notin \mathsf{Odd}(p(u))$. Moreover, $u \notin \lambda^{-1}(\{Z\}) \Leftrightarrow X \in \lambda_u \Rightarrow u \in \mathsf{Odd}(p(u))$, thus $\mathsf{Odd}(p(u)) \setminus ((O \cup \lambda^{-1}(\{Z\})) = \{u\} \setminus \lambda^{-1}(\{Z\})$. Similarly $p(u) \setminus (O \cup \lambda^{-1}(\{X\})) = \{u\} \setminus \lambda^{-1}(\{X\})$.

By induction, for a given $u \in O^c$, assume the property is satisfied for all $v \in O^c$ s.t. $u < v$ which implies:

$$\begin{aligned}
\mathsf{Odd}(p_X(v)) \setminus (O \cup \lambda^{-1}(\{Z\})) &= \emptyset \\
\mathsf{Odd}(p_Z(v)) \setminus (O \cup \lambda^{-1}(\{Z\})) &= \{v\} \setminus \lambda^{-1}(\{Z\}) \\
p_X(v) \setminus (O \cup \lambda^{-1}(\{X\})) &= \{v\} \setminus \lambda^{-1}(\{X\}) \\
p_Z(v) \setminus (O \cup \lambda^{-1}(\{X\})) &= \emptyset
\end{aligned}$$

$$\begin{aligned}
&p(u) \setminus (O \cup \lambda^{-1}(\{Z\})) = g(u) \setminus (O \cup \lambda^{-1}(\{Z\})) \oplus \\
&\left(\bigoplus_{\substack{v \in \mathsf{Odd}(g(u)) \setminus \{u\} \\ \text{s.t.} X \in \lambda_v}} p_Z(v) \setminus (O \cup \lambda^{-1}(\{Z\})) \right) \oplus \left(\bigoplus_{\substack{v \in g(u) \setminus \{u\} \\ \text{s.t.} Z \in \lambda_v}} p_X(v) \setminus (O \cup \lambda^{-1}(\{Z\})) \right) \\
&= g(u) \setminus (O \cup \lambda^{-1}(\{Z\})) \oplus \left(\bigoplus_{\substack{v \in g(u) \setminus \{u\} \\ \text{s.t.} Z \in \lambda_v}} \{v\} \setminus (O \cup \lambda^{-1}(\{Z\})) \right) \\
&= g(u) \setminus (O \cup \lambda^{-1}(\{Z\})) \oplus (g(u) \setminus \{u\}) \setminus (O \cup \lambda^{-1}(\{Z\}) \\
&= \{u\} \setminus (O \cup \lambda^{-1}(\{Z\})) = \{u\} \setminus \lambda^{-1}(\{Z\})
\end{aligned}$$

Similarly,

$$\begin{aligned}
&\mathsf{Odd}(p(u)) \setminus (O \cup \lambda^{-1}(\{Z\})) = \mathsf{Odd}(g(u)) \setminus (O \cup \lambda^{-1}(\{Z\})) \oplus \\
&\left(\bigoplus_{\substack{v \in \mathsf{Odd}(g(u)) \setminus \{u\} \\ \text{s.t.} X \in \lambda_v}} \mathsf{Odd}(p_Z(v)) \setminus (O \cup \lambda^{-1}(\{Z\})) \right) \oplus \left(\bigoplus_{\substack{v \in g(u) \setminus \{u\} \\ \text{s.t.} Z \in \lambda_v}} \mathsf{Odd}(p_X(v)) \setminus (O \cup \lambda^{-1}(\{Z\})) \right) \\
&= \mathsf{Odd}(g(u)) \setminus (O \cup \lambda^{-1}(\{Z\})) \oplus \left(\bigoplus_{\substack{v \in \mathsf{Odd}(g(u)) \setminus \{u\} \\ \text{s.t.} X \in \lambda_v}} \{v\} \setminus (O \cup \lambda^{-1}(\{Z\})) \right) \\
&= \mathsf{Odd}(g(u)) \setminus (O \cup \lambda^{-1}(\{Z\})) \oplus (\mathsf{Odd}(g(u)) \setminus \{u\}) \setminus (O \cup \lambda^{-1}(\{Z\}) \\
&= \{u\} \setminus (O \cup \lambda^{-1}(\{Z\})) = \{u\} \setminus \lambda^{-1}(\{Z\})
\end{aligned}$$